Novel Order preserving encryption Scheme for Wireless Sensor Networks

Elie Khoury, Maguy Medlej, Chady Abou Jaoude, Christophe Guyeux

Novel Order preserving encryption Scheme for Wireless Sensor Networks

Elie Khoury, Maguy Medlej and Chady Abou Jaoude
TICKET Lab, Faculty of Engineering
Antonine University, Hadat-Baabda, Lebanon
elie.akhoury@ua.edu.lb, maguy.medlej@ua.edu.lb,
chady.aboujaoude@ua.edu.lb

Christophe Guyeux
Femto-ST Institute, UMR 6174 CNRS
University of Bourgogne Franche-Comté, France
christophe.guyeux@univ-fcomte.fr

***Abstract*—An Order-Preserving Encryption (OPE) scheme is a deterministic cipher scheme, whose encryption algorithm produces cipher texts that preserve the numerical ordering of the plain-texts. It is based on strictly increasing functions. It is a kind of homomorphic encryption where the homomorphic operation is order comparison. This means that comparing encrypted data provides the exact result than comparing the original data. It is attractive to be used in databases, especially in cloud ones as a method to enhance security, since it allows applications to perform order queries over encrypted data efficiently (without the need of decrypting the data). Wireless sensor network is another potential domain in which order preserving encryption can be adopted and used with high impact. It can be integrated with secure data aggregation protocols that use comparison operations to aggregate data (MAX, MIN, etc.) in a way that no decryption is being performed on the sensor nodes, which means directly less power consumption. In this paper, we will review many existing order-preserving encryption schemes with their related brief explanation, efficiency level, and security. Then, and based on the comparative table generated, we will propose a novel order-preserving encryption scheme that has a good efficiency level and less complexity, in order to be used in a wireless sensor network with an enhanced level of security.**

Keywords*—Order preserving encryption, security, wireless sensor networks.

I. Introduction

Wireless Sensor Networks (WSNs) are still one of the most challenging research areas in our present time. They consist of a system of sensor nodes that communicates using wireless communications distributed in either a safe or an unfriendly environment. The most challenging part of these nodes is their restriction in terms of resources, since they have low battery power, limited memory and computation capacity. WSNs are used in various fields like agriculture, medicine, the army, VANet, etc. [26]. Hence, the usage of the WSNs in these vast and critical fields, has obliged the security part to become one of the major aspects to be enhanced, alongside minimizing energy consumption.

As a solution for the energy consumption and to enhance the wireless sensor network vitality status, data aggregation is being adopted as an efficient technique to enhance the battery life of each node by minimizing the processing operation, and reducing the amount of data being sent between the nodes. Hence, sensor nodes send their values to the aggregators, then the aggregators collect the data received and send them to the base station. Since some wireless sensor network applications are used in military fields and are being dispersed in hostile and non-controllable zones, security of the WSNs has become a very essential part to be strengthened and enhanced. In addition, and since WSNs are being used in critical public sectors like VANet and medical fields, security is becoming a complete requirement since if any of the security triangle, confidentiality, integrity, or availability is compromised, the whole application will no longer be reliable.

Based on all the previous interpretations [9], [21], securing the sensed data aggregated from the beginning to the end is essential by adopting an end-to-end encryption. In addition, using homomorphic encryption with different homomorphic operations (addition, multiplication, comparison, etc.) will enhance the sensor battery lifetime, since no decryption/encryption needed on the aggregated node is required to perform data aggregation operations based on the chosen data aggregation protocol.

Order-preserving encryption (OPE) is a kind of homomorphic encryption where the homomorphic operation is order comparison. This means that comparing encrypted data provides the exact result than comparing the original data. In summary, if $x < y$, then $f(x) < f(y)$. Its rewards is that systems can perform order operations on cipher texts in the same way as on plaintexts [1], [2], [3], [5], [12]. Because of the status of the wireless sensor nodes, in terms of low battery level, limited memory, and computation capacity, performing order operation on cipher text is very efficient. Indeed, it allows the node to use the encrypted data as it is (without decryption), and to perform order operations like equality and range comparison as well as the MAX, MIN, COUNT, GROUP BY, and ORDER BY computation.

In this paper, we will provide a brief summary regarding the most known order preserving encryption schemes used in several domains with their respective efficiency, security, and complexity levels. Then, based on the comparative table generated, we will introduce a novel order-preserving encryption scheme that can work in a wireless sensor network. This novel OPE scheme will be based on a low complexity level encryption algorithm (O (log(n))), a high efficiency level compared to other OPE schemes, and a high security level since the symmetric key generated will be periodically updated based on a random T period of time. For future work, this novel order preserving encryption will be tested and enhanced in every single part.

The remainder of this paper is organized as follows : In Section II, previous works on order preserving encryption in other fields and sectors are described. An optimized scheme that has a better performance, less complexity, and enhanced security is proposed in Section III. This latter can fit in wireless sensor networks. The simulation outcomes and results are shown and analyzed in Section IV. The conclusion and future work are finally summarized in Section V.

II. RELATED WORK

There has been a serious quantity of work on OPE schemes, see, *e.g.*, [1], [2], [3], [4], [5], [6], [7], [8], [10], [14], [15], [16], [17], [18], [19], [22], [23], [24], [25]. They either provide a good efficiency but low security or the opposite, as will be proven later. In this area, we present a detailed overview of different typical known types of OPE schemes with their related advantage/disadvantage, alongside with the parameters chosen to evaluate the OPE Scheme, i.e., efficiency level, security level, complexity level, and the order of comparison.

The premier provably-secure OPE scheme was created by Boldyreva [7]. It provided the first formal treatment of security. Like any other OPE, Boldyreva's order-preserving encryption algorithm forms a monotonically increasing curve. The BCLO (Boldyreva, Chenette, Lee, and O'Neill) scheme was introduced based on a sampling algorithm for the hypergeometric probability distribution. This Hypergeometric Distribution (HG) is a discrete probability distribution that represents the number of successes in a series of draws from a finite population without replacement. In order to meet the security notion of an OPE scheme looks "as-random-as possible", the encryption method of the BCLO scheme uses 2 algorithms (LazySample and LazySampleInv) that examine a random order-preserving function from domain D to range R and its inverse, respectively (plaintext-space D and ciphertext-space R). In other words, any order-preserving function g(.) from domain D= $\{1 \dots M\}$ to range R= $\{1 \dots N\}$ can be particularly defined by a combination of M out of N ordered items.

With this approach, encryption function is based on hypergeometric distribution maps plaintexts from the set [1, 2, ..., M] to the set [1, 2, ..., N], where $N > M$. The cipher texts generated from this scheme is in order and associated correspondingly with plaintext numbers. This scheme has a low-efficiency level, but with a medium security standing that makes it different from other low-security levels. To reduce the computational cost of the BCLO scheme of [7], Yum used the probabilistic middle gap instead of the Euclidean middle one [10]. Simulations show that the proposed method is effective for various distributions, especially for distributions with small variance. This scheme has a low to medium efficiency level with a same medium security standing of the Boldyreva, 2009 [7].

In 2011, Boldyreva [3] provided a promising extension, the modular order-preserving encryption (MOPE), that enhances the security level of the basic OPE by inserting a secret modular offset to each data value before encrypting it. MOPE improves the security of OPE in a sense, as it does not leak any information about plaintext location. But later on, it was proven [3] that OPE schemes cannot satisfy standard notions of security, such as indistinguishability against chosen-plaintext attack (IND-CPA), since they lack the ordering information of the plaintexts. If an adversary knows plaintexts p1, p2 and corresponding ciphertexts c1, c2, and c, such that c1<c<c2, it is obvious that the plaintext for c lies in the interval (p1, p2). In addition, the adversary can always discover the decryption function in some approximation, for instance, using linear interpolation. In [20], they introduced a new appropriate security model for MOPE that has a significant security improvement over the basic OPE. The complexity of the algorithm used in [3], [20] is O (n), but has low efficiency level and medium security (it leaks some data).

Liu and Wang [5] presented a simple linear scheme, easy to use, that is based on a linear expression. In addition to the linear expression, a random noise is added to the initial plaintext to enhance the security level. In details, the linear order preserving encryption scheme proposed in [11] is built over the expressions of the form $y = a \times x + b + noise$, where x is a plaintext, a and b are secret coefficients, y is the ciphertext, and noise is a randomly selected value. To guarantee the order preserving property, it is required that $a > 0$ in the linear expression and that noise is randomly selected from some particular range. To determine the range of noises, the sensitivity of input values is needed. The sensitivity characterizes the minimal difference between two plaintexts, i.e., if the plaintexts belongs to Z, then sensitivity is equal to 1. Another example, if the sensor collects the weather degree, the sensed values can be 35.5, 35.6, 35.7, etc. So the minimal difference between one degree and another one is 0.1, which leads to a sensitivity of 0.1.

This OPE scheme is information-theoretically secure, since attackers cannot get enough information to solve the linear equations over the input values. But, as discovered later on, the linear OPE scheme might be vulnerable when there are too many duplicates in plaintexts. For each plaintext value v, we generate an encrypted value v' by using the linear function $Enc(x) = ax + b + noise$. The advantage of this solution is the efficiency level, but it has low security.

Until now, the only ideal security OPE scheme is the mutable order-preserving encoding (mOPE) implemented by Popa [2], where the ciphertexts reveal nothing except the order of the plaintext values. The mOPE run by building a balanced search tree that includes all of the plaintext values encrypted by the application in the database side. The interactive encryption protocol, with a small number of interactions, changes over time the ciphertexts for a small number of plaintext values. These operations in database side can be executed by User Define Functions (UDFs).

In summary, it requires the database server to retain additional information and perform comparison or range query by UDFs. However, order operations will no longer be executed directly on the ciphertext. It will affect the efficiency and make this scheme unsuitable for some cases, i.e., for wireless sensors networks. More specifically, experiments show that it has a poor efficiency, extra storage, no direct comparison on ciphertexts, and its execution time of encryption is very high. On the other Hand, in terms of security, the Popa's scheme achieves ideal-security. Let us finally note that algorithm complexity is of the magnitude of O (n log n).

In order to address the vulnerability of the previous linear

Scheme	Efficiency	Security	Complexity	Order of comparison
Agrawal, 2004 [17]	Medium	Low	O(n)	Direct
Boldyreva, 2009 [7]	Low	Medium	O(n)	Direct
Agrawal, 2009 [1]	Medium	Medium	O(n)	Direct
Boldyreva, 2011 [3]	Low	Medium	O(n)	Direct
Liu, 2012 [5]	High	Low	O(n)	Direct
Popa, 2013 [2]	Low	High	O(n log n)	UDFs
Liu, 2013 [8]	Medium	Medium	$O(n^2)$	Direct
Dyer, 2017 [13]	High	Medium	O(1)	Direct

TABLE I. COMPARISON BETWEEN TYPICAL OPE SCHEMES

OPE schemes when there are too many duplicates in plaintexts, Liu and Wang [8] presented a nonlinear OPE that can be calculated from the expression $y = a \times f(x) \times v + b + noise$, where a, $f(x)$, and b are kept secret, with the following requirements satisfied:

$$a > 0, \tag{1}$$

$$noise \in [0, a * f(v + sens) * (v + sens) - a * (f(v) * v)], \tag{2}$$

$$f(x) > 0 \text{ for } x \neq 0, \tag{3}$$

$$f(x_1) \geq f(x_2) \text{ for } x_1 > x_2 > 0. \tag{4}$$

The advantage of this method is that it is more secure than the previous one. The disadvantage is that it is less efficient since the encryption algorithm is more complex.

A new simple OPE model has been proposed by Liu in 2014 [4], that uses message space expansion and nonlinear space split for hiding the frequency and the data distribution. This research was based on Liu's 2013 scheme, and works as follows. Firstly, the original message space is randomly split into successive intervals with different lengths. Secondly, an extended ciphertext space is selected and split into the same number of intervals. Finally, some nonlinear mapping functions are used to map the original element into another one in the extended message space ($Enc(x) = ax + b + noise$). This scheme is constructed by some linear mathematical functions used by Liu and Wand, 2013. In terms of security, this scheme can achieve to face ciphertext-only attacks. Furthermore, this scheme uses message space expansion and nonlinear space split to cover data distribution and frequency, and thus can resist to statistical attacks.

Finally, in 2017, J. Dyer [13] proposed a new simple randomized order-preserving encryption scheme based on the general approximate common divisor problem (GACDP). It is based on computational hardness primitive. The results show that this scheme is very efficient compared to other OPE schemes, since there are O(1) arithmetic operations for both encryption and decryption. Note finally that the security level of this scheme is classified as medium.

Table I displays the comparison between some typical OPE schemes. The compared parameters are the efficiency level, the security, the complexity, and the order of comparison. About the security, only Popa [2] provides a high level of security compared to others OPE schemes, since the ciphertexts reveal nothing except for the order of the plaintext values (ideal-security). About the efficiency, we can see that security and efficiency are always contradictory: the most secure is the less efficient. Dyer [13] and Liu [5] using an O(1) and O(n) arithmetic operations respectively for encryption and decryption have the best efficiency compared to others.

In summary, and since we are targeting the integration of OPEs in wireless sensor networks, our approach is to use an efficient OPE scheme in order to be applicable in the WSN (less complexity = less resources usage = more efficient). In addition, the more the OPE scheme is secure the better we are, for that purpose our tactic will be to enhance the security level for the selected OPE.

III. PROPOSAL AND IMPLEMENTATION ENVIRONMENT

A. Order Preserving Encryption standard Scheme

An order-preserving encryption (OPE) scheme with plaintext-space [M] and ciphertext space [N] is a tuple of algorithms $OPE = (Kgen, Enc, Dec)$ where:

- The randomized key-generation algorithm Kgen outputs a key, $K(a, b)$.
- The deterministic encryption algorithm Enc, inputs a key K, a plaintext m and outputs the ciphertext c.
- The deterministic decryption algorithm Dec, inputs a key K, a ciphertext c and outputs the plaintext m.

In addition to the usual requirement that Dec(Enc(K, m)) = m, for every plain-text m and key K, we require that $m1 < m2$ if and only if $Enc(K, m1) < Enc(K, m2)$ for all plaintexts m1, m2 and every key K. Notations are summarized below.

m	⇒ plain-text
c	⇒ cipher-text
K	⇒ the Encryption key, belonging into $k = \{(a, b), a, b \in \mathbb{Z}^+\}$
Enc	⇒ Encryption algorithm that contains the procedure OPEEnc
Dec	⇒ Decryption algorithm that contains the function OPEDec

B. Secure Data aggregation in Wireless Sensor Networks (end-to-end encryption) using OPE scheme.

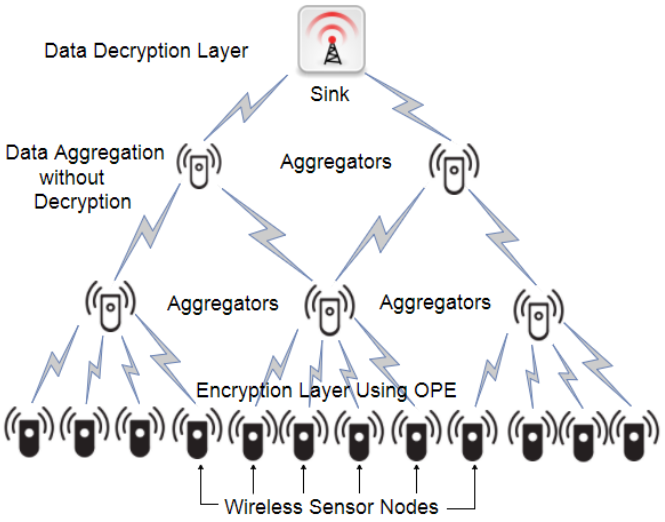

Fig. 1. Secure Data aggregation in Wireless Sensor Network (end to end encryption) using Order-Preserving Encryption scheme

The system model shown in Figure 1 works using three stages:

- **Stage1:** Encryption phase
  Sensors encrypt the data detected by using OPE with a master secret key shared by all the wireless nodes in the network. The encrypted data set is sent to the aggregator.
- **Stage2:** Aggregation - Verification
  The aggregator calculates/analyses/compares the aggregates of the encrypted data using order operations like equality/range comparison as well as the MAX, MIN, COUNT, GROUP BY, and ORDER BY. It then sends the results to the Base Station: no need for decryption.
- **Stage3:** Decryption phase
  The base station decrypts the encrypted data set and calculates the plaintexts of the aggregates.

C. Proposing our novel OPE Scheme.

Based on Table I, OPE encryption based on both the linear expression y = ax+b and the logarithm expression $c = a * log(m + b)$ have the best efficiency, since their complexity levels are low: linear expression O(n) and logarithm expression O(log(n)). They are very suitable to be used in a wireless sensor network, especially for the O(log(n)) complexity, which is obviously better than the O(n) one.

So, as a first step, we will use the logarithm expression, $y = a\ log(x+b)$ as the base of our OPE system, with $a, b \in \mathbb{Z}^+$ and $x+b > 0$. But this cryptosystem, like many others, will be vulnerable to the chosen-plaintext attack. And, even if we add to this expression some random noise, this cryptosystem will be less vulnerable. But, it will still be defenseless against the chosen-plaintext attack, and the key (K) can be revealed. For this reason, updating a and b on a random period can minimize the era time of the key k(a,b), so any chosen-plaintext attack cannot cause any serious damage to this OPE scheme, since the key will be generated on a random period. In a nutshell, our proposed OPE is very efficient and is mainly more secure compared to other OPE schemes.

To implement this novel OPE scheme, our algorithm will be divided into 3 parts, which can be written as follows: OPE = (KeyGen, OPEEnc, OPEDec)

- **Step1:**
  The target of this algorithm is to set up the exact parameters to generate the encryption key, in addition to defining the period of time it takes p to regenerate a new key.
  Algorithm 1 Key Generation
  1: Procedure KeyGen(a,b)
  2: Input (a,b) // $\{(a, b), a, b \in \mathbb{Z}^+\}$, random input
  3: Return K
  4: End Procedure
  5: input p // p=period, the period of time before a new key generation

- **Step2**
  The target of this algorithm is to encrypt the plaintext data m and outputs its OPE cipher text. To encrypt m, we need to have the key generated k as an input.

  Algorithm 2 OPE Encryption
  1: Procedure OPEEnc (m,k)
  2: $m \in Z^+$
  3: Input (m,K)
  4: c = a*log(m+b) // This cryptosystem is highly efficient, since the encryption function is logarithmic (O(log(n))
  5: Return c
  6: Threshold T = T+1
  7: If T == p then KeyGen(a,b) // a,b should be random new numbers, p = period already defined
  8: End Procedure

- **Step3**
  The target of this algorithm is to decrypt the encrypted data y and outputs its OPE plaintext.

  Algorithm 3 OPE Decryption
  1: Procedure OPEDec (c,K) // inverse of the procedure OPEEnc
  2: $m = (a\ log(c + b))^{-1}$ // the exponential function is the inverse function of a logarithm function $\Rightarrow$ it will be complex $\Rightarrow$ more battery usage $\Rightarrow$ it will be performed on the base station only since we are considering working in an end-to-end encryption
  3: Return m
  4: End Procedure

As a programming language, Matlab was used to perform the simulation. The algorithms were tested on a virtual machine that has the following specifications: i3-7100 CPU, 8GB DDR4, and 1TB HDD 7200 RPM. The VM has Windows 8.1 OS running on it. This VM will be matched to a next generation wireless sensor node.

D. Strategy Selection

Based on the comparative Table I, we selected Dyer [13] OPE scheme that is based on the general approximate common divisor problem (GACDP) as the baseline of our simulation. Our selection was based on the efficiency level of this scheme compared to other OPE schemes, since there are O(1) arithmetic operations for encryption and decryption. In addition of its efficiency, this scheme has a good security level, since it produces larger cipher texts, ~ 3.67 times the number of bits of the plaintext, and has minimal impact on the running time. Based on our experiment results, we discovered that the efficiency of this scheme makes it fit for usage in wireless sensor networks.

The security level of our OPE scheme is definitely better, because the symmetric encryption key will be updated on a random period, so it can minimize the era time of the key k(a,b). We will now test the efficiency level of our code, and prove that our Olog(n) code is also faster.

IV. Experimental Results

To evaluate our novel OPE scheme in practice, we performed an experiment by encrypting 100 times both OPE

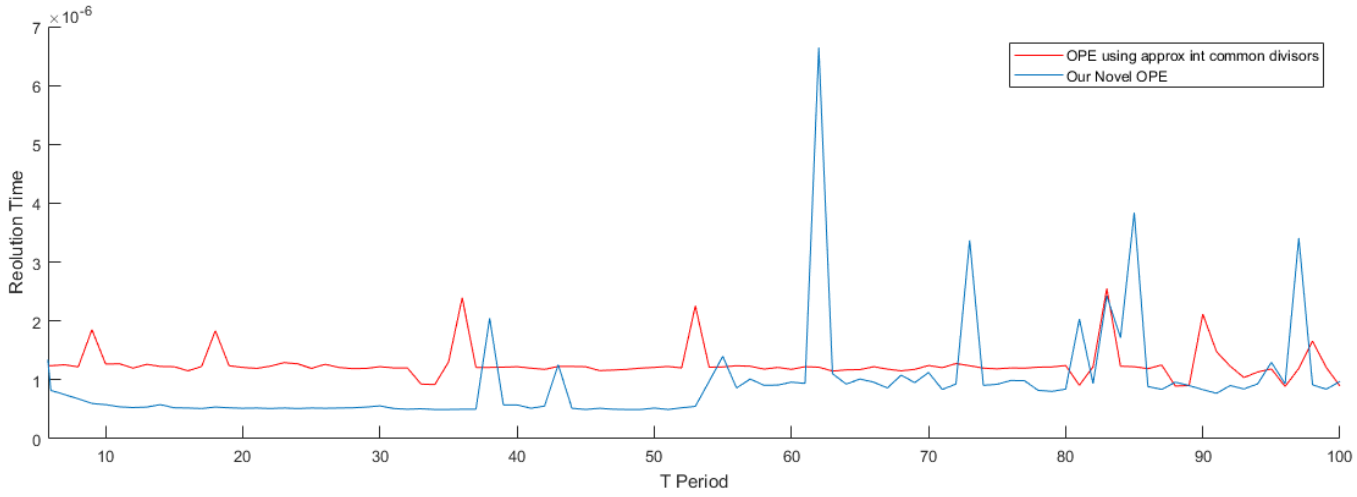

Fig. 2. Comparison of time resolution - Simulation 1

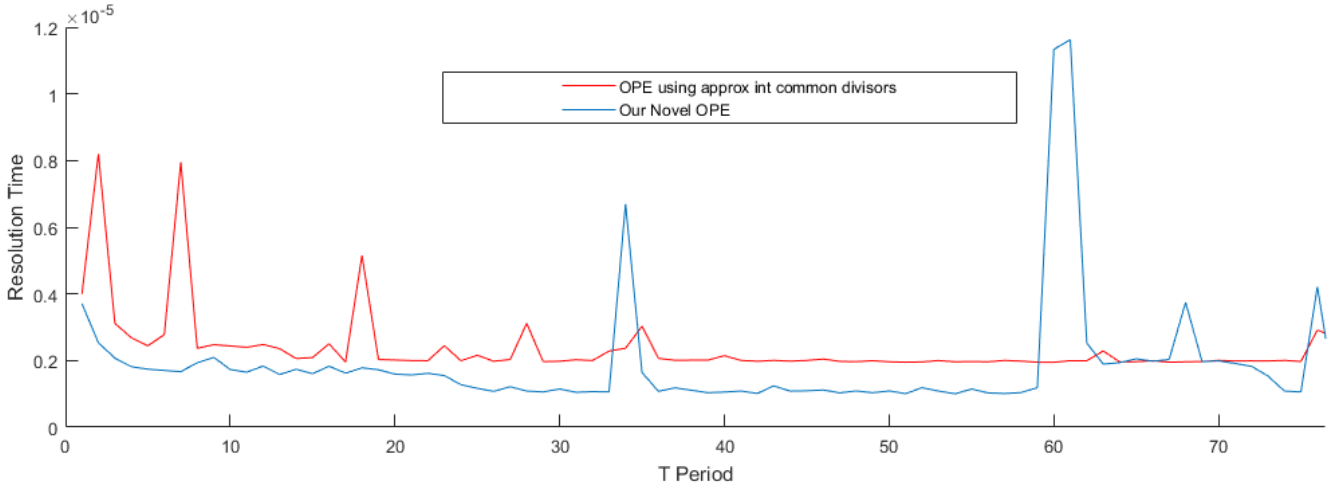

Fig. 3. Comparison of time resolution - Simulation 2

schemes; the first one (in red) represents the general approximate common divisor problem (GACDP) and the second one (in blue) is our novel OPE scheme. The simulation is based on the algorithm and the strategy already mentioned previously in the article. Note that both algorithms will be executed separately. The parameters needed for the key generation (a, b and p) will be selected manually or randomly.
Figure 2 and Figure 3 represents two simulations samples that have different random key generation parameters(a,b and p).

As a first observation, and based on several simulations and testing performed on the key generation, we noticed that the resolution time of our novel OPE scheme is faster than the (GACDP) scheme for the period between $0 < T < 60$ as visualized in the Figure 2 and Figure 3.
As a second observation, we can detect that after the period of 60, $T > 60$, the resolution time of our novel OPE will start to be similar than the OPE of the approximate common divisor problem (GACDP), (see Figure 2 and Figure 3).
As an outcome, our novel OPE resolution time code is faster than the (GACDP) scheme when the period is less than 60, and after 60 it starts to decelerate but in the other hand more secure for the reason that the key is being changed and generated on a random basis, strengthening the security level of our scheme and harden the key detection by any attacker and the bigger the period is, the greater the security level is.

V. Conclusion and Future Work

In this article, we provided a sharp description of various order preserving encryption schemes. In addition, various design issues such as data confidentiality, data integrity, efficiency level, and security of these OPE schemes have also been discussed and evaluated. And, based on the data generated in the comparative table of this paper, we have proposed a novel secure order preserving encryption scheme that can suit a wireless sensor network, in terms of efficiency, complexity, and security. The implemented OPE scheme is based on a logarithm encryption function which makes the scheme very efficient and less complex compared to other OPE schemes. In addition, and to enhance the security level of this OPE scheme, the symmetric encryption key is updated based on a T period of time, so it can minimize the era of the key k(a,b). In consequence, it is very hard for any attacker to discover the

key. And even if the key is sorted out, it will be useless since it will have expired based on period already specified. After performing some experiments, we have proven that our new OPE scheme is faster, more efficient, and most of all more secure. In addition, and after fine tuning the results, we have found that T between 0 and 60 is the best range. Beyond 60, our scheme starts losing its efficiency compared to the other OPE Scheme.

As a future work, the efficiency level of the adopted OPE cryptosystem with improvement of the bundle of algorithms used (keyGen, OPEEnc, OPEDec) can be optimized. In addition, a smart key generation updater could be based on a machine learning algorithm that can detect the rate of live attacks. As a consequence, the rate of the key generation will be optimized in a secure and efficient way.

REFERENCES

[1] D. Agrawal, A. El Abbadi, F. Emekci, and A. Metwally. Database management as a service: Challenges and opportunities. In ICDE, 2009.

[2] Popa RA, Li FH, Zeldovich N. An ideal-security protocol for order-preserving encoding. In: 2013 IEEE symposium on IEEE Security and Privacy (S & P), 2013.

[3] Boldyreva A, Chenette N, O'Neill A. Order-preserving encryption revisited: improved security analysis and alternative solutions. Advances in Cryptology-CRYPTO 2011. Berlin, Heidelberg: Springer; 2011, p. 578–95.

[4] Liu Z, New order preserving encryption model for outsourced databases in cloud environments. Journal of Network and Computer Applications, 2014.

[5] Liu D, Wang S. Programmable order preserving secure index for encrypted database query. Proceedings of the 5th IEEE International Conference on Cloud Computing, Honolulu, Hawaii, USA, 2012; 502–509.

[6] Lovepreet kaur and Jyoteesh Malhotra, "Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Future Generation Communication and Networking Vol. 8, No. 4 (2015), pp. 81-88.

[7] Boldyreva A, Chenette N, Lee Y, O'Neill N. Order-preserving symmetric encryption. Advances in Cryptology-EUROCRYPT 2009. Berlin, Heidelberg: Springer; 2009.p. 224–41.

[8] Liu D, Wang S. Nonlinear order preserving index for encrypted database query in service cloud environnements. Concurrency and Computation Practice and Experience 25(13), September 2013.

[9] Jacques M. Bahi, Christophe Guyeux, Abdallah Makhoul "Two Security Layers for Hierarchical Data Aggregation in Sensor Networks", Article in International Journal of Autonomous and Adaptive Communications Systems, January 2011.

[10] D. Yum, D. Kim, J. Kim, P. Lee, and S. Hong. Order preserving encryption for non-uniformly distributed plaintexts. In Intl. Workshop on Information Security Applications, 2011.

[11] Ke Li, Weiming Zhang, Ce Yang, and Nenghai Yu. Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search. DOI 10.1109/TIFS.2015.2435697, IEEE Transactions on Information Forensics and Security.

[12] C. Wang, N. Cao and K. Ren, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions 23(8), pp. 1467-1479, 2012.

[13] James Edward Dyer, Martin Dyer, and Jie Xu, "Order-Preserving Encryption using approximate integer common divisors", 2017.

[14] H. Kadhem, T. Amagasa, and H. Kitagawa. MV-OPES: Multivalued-order preserving encryption scheme: A novel scheme for encrypting integer value to many different values. IEICE Trans. on Info. and Systems, E93.D(9), 2010.

[15] H. Kadhem, T. Amagasa, and H. Kitagawa. A secure and efficient order preserving encryption scheme for relational databases. In International

[16] S. Lee, T.-J. Park, D. Lee, T. Nam, and S. Kim. Chaotic order preserving encryption for efficient and secure queries on databases. IEICE Trans. on Info. and Systems, E92.D(11), 2009.

[17] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Order preserving encryption for numeric data. In ACM SIGMOD, 2004.

[18] V. Kolesnikov and A. Shikfa. On the limits of privacy provided by order-preserving encryption. Bell Labs Technical Journal,17(3), 2012.

[19] Mithun Acharya, Joao Girao, and Dirk Westhoff. Secure Comparison of Encrypted Data in Wireless Sensor Networks

[20] Charalampos Mavroforakis, Nathan Chenette, Adam O'Neill, George Kollios, and Ran Canetti. Modular Order-Preserving Encryption, Revisited

[21] Christophe Guyeux, Abdallah Makhoul, Ibrahim Atoui, Samar Tawbi, and Jacques M. Bahi. A Complete Security Framework for Wireless Sensor Networks: Theory and Practice, january 2015

[22] Minkyu KIM, Je Hong Park and Dongyoung ROH. Comment on the Security of an Order-Preserving Encryption Scheme Using Pseudo-Random Function, 2016

[23] Zheli Liua, Xiaofeng Chenb, Jun Yanga, Chunfu Jiaa and Ilsun You. New order preserving encryption model for outsourced databases in cloud environments, 2016.

[24] Harshali Kanherkar, Ashwini Ingale, Sonali Kanse, Pallavi Naykinde, Prof. Belsare P.P. A Simplified Approach on Security Analysis Using Probabilistic Order Preserving Encryption Based on Cloud Data Search, 2017.

[25] Yanguo Peng, Hui Li, Jiangtao Cui, Junwei Zhang, Jianfeng Ma and Changgen Peng. hOPE: improved order preserving encryption with the power to homomorphic operations of ciphertexts, 2017.

[26] Tannoury, Anthony and Darazi, Rony and Guyeux, Christophe and Makhoul, Abdallah. Efficient and accurate monitoring of the depth information in a Wireless Multimedia Sensor Network based surveillance. In SENSET 2017, First International Conference on Sensors, Networks, Smart and Emerging Technologies. Beirut, Lebanon, September 2017.